AU/ACSC/2012

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

WEB OF DECEPTION: SOCIAL MEDIA AND IMPLICATIONS FOR MILITARY DECEPTION

by

Patrice L. Lyons, Maj, USAF

A Writing Assessment Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Mr. Marco A. Burgos

Maxwell Air Force Base, Alabama

December 2012

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

TABLE OF CONTENTS

Page

ABSTRACT

This paper examines the threats and opportunities for military deception created by social media. Overall, the paper asserts that although there are barriers, social media can and should be used for military deception operations. Furthermore, comprehensive counterdeception strategies should be developed. Using recent examples, it describes how social media is currently being used for deception by multiple actors and illustrates the need for more agile counterdeception efforts. It also explores opportunities for the use of social media by the Department of Defense in its own military deception operations. A review of doctrinal and legal issues highlights the potential barriers that exist in the use of social media in military deception and counterdeception, and recommendations for future planning and operations are provided. With looming Department of Defense budget cuts, integration of military deception and social media can be an inexpensive, but lucrative force multiplier.

Introduction

Social media has revolutionized the spread of information. These technologies, which allow online communication through user-generated content, exist in multiple forms on multiple platforms. They include text, picture, and video formats in blogs, collaborative projects, and social networking sites.[1] Reporting of events in one part of the world no longer depends on traditional media to pick it up and process it. In addition, social media tools have transformed the spread of information from one-way conversations via radio, newspaper, and television to interactive conversations open to millions of people. Currently, there are more than one billion Facebook users, over 340 million Tweets per day, and 72 hours of video uploaded to YouTube every minute.[2]

Military organizations have not gone untouched by the information revolution created by the new digital media. On 14 November 2012, the Israel Defense Force (IDF) first announced attacks on the Gaza Strip via their Twitter account, not through a press conference. This action set the stage for the days to come. In addition to rocket attacks and gunshots, a non-kinetic "social media war" ensued. While the IDF was considered to have a well-organized machine versus Hamas, nonstop updates were provided by both sides on Twitter and other social media sites. Civilians even got involved, adding their own inputs on Twitter, YouTube, and Facebook. [3] The winner of the propaganda war is up for debate, but it certainly depicted an idea of how future operations may look.

While not a smooth process, the Department of Defense (DOD) has also begun to integrate these new platforms into their information operations (IO). In 2009, the DOD performed a review on social media and examined the potential benefits versus security risks.[4] As a follow-up in 2010, Deputy Defense Secretary William J. Lynn issued a memorandum

allowing the responsible use of internet-based capabilities, including social media tools, on DOD networks.[5]

The DOD is increasingly embracing social media use, with hundreds of official sites across more than 16 different platforms.[6] Efforts are mostly focused in the Public Affairs (PA) arena, as ongoing concerns regarding security and the openness of these forums have limited social media use in other areas.[7] However, as one of the core IO capabilities, military deception (MILDEC) offers a powerful venue to leverage the new social media technologies. [8] Joint Publication 3-13.4, *Military Deception*, defines MILDEC as "actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission."[9] Although there are legal and doctrinal concerns, the rapid explosion of social media presents a new weapon for the DOD in executing and supporting MILDEC operations, and as recent events demonstrate, a new threat that requires exploration of more agile counterdeception methods.

A Deception Threat Exists

With the increase in capabilities in the information age, it was believed by some that MILDEC operations could no longer be carried out. The capabilities were expected to create omniscient actors. However, this has not proven to be true. There are many examples that show how deception is still possible and how tactics have adapted to the newer technologies.[10] For example, in Desert Shield, the intense media coverage of the amphibious operations in the Gulf of Oman only enhanced the deception operation.[11] "Deception's target remains the same, only the pathways to the target have changed."[12]

The use of social media for deception and disinformation has already shown up in recent conflicts. For example, in August 2012, a Reuters Twitter account was hacked by supporters of Syrian President Bashar al-Assad and eluded to a rebel defeat in Aleppo. The next day, an account controlled by Syrian rebel forces reported the death of President al-Assad. After a continuation of false posts and inaccurate reports, Reuters' system was temporarily shut down.[13] Furthermore, in the most recent conflict in Gaza, pictures of dead children from the Syrian conflict were posted on Twitter and Facebook, with false reports suggesting that the casualties were from rocket attacks in the area.[14] In both examples, the information quickly proved to be false, and it appeared the efforts did not provide either side with an advantage on a tactical, operational, or strategic level. However, they clearly illustrate how deception tactics are finding their way into social media.

There are instances where deception using social media is proving effective. In Mexico, crime organizations have used Facebook and Twitter to spread false information and warnings about violence, diverting police attention. This requires officers to not only respond to false reports, but also to expend effort counteracting panic and chaos caused by the rumors.[15] Because violence is typical in many areas in Mexico, crime organizations can take advantage of this preconditioning and set the populace and police up for a reaction.

The United States (US) is not immune to exposure to deception through the new media avenues. On 26 March 2006, the United States fell victim to the almost instantaneous reporting cycle the new media permits. During Operation Valhalla, US and Iraqi Special Forces units tracked down and defeated Jaish al-Mahdi (JAM) death squad fighters who had brutally murdered several civilians and Iraqi troops. In the encounter, the US and Iraqi forces killed 16-

17 JAM fighters, captured approximately the same number, destroyed a weapons cache, and rescued a hostage. Overall, it was a successful operation.

However, less than one hour after they left the site, pictures from a cell phone camera were posted on the internet that portrayed a very different story. Someone had repositioned the bodies and moved the guns so that it appeared as though the JAM fighters were killed during prayer. A press release accompanied the pictures, claiming American troops had murdered the men during prayer at a mosque. The traditional media jumped on the story right away, and it grabbed the attention of the American public. Although "before" pictures by US forces did exist, it took 70 hours for a briefing to occur, and a month-long investigation still ensued. During this investigation, the US Special Forces unit was essentially non-operational. Whether or not this was originally meant as a propaganda method targeted to local audiences, this deception ultimately had an impact on the US public and decision makers, temporarily degrading operational capability.[16]

The Need for Counterdeception

Even if the US military chooses not to use social media as a technical means in MILDEC operations, it cannot ignore the need for counterdeception efforts in regards to social media use by current or future adversary forces. The Taliban is using Facebook for recruiting, to incite terrorist attacks, and to spread false information.[17] China, while highly censored and not operating on traditional Western and Asian sites, has robust social media use by its population.[18] Furthermore, the fastest growth in the use of new media technologies is in regions at risk for instability, the probable battlefronts in the future.[19]

Just as traditional media was used for disinformation and black propaganda in the past, new media will be used in the future. However, the new social media platforms remove a level of

filtering for accuracy that should normally be performed by traditional media. It is now a world of instantaneous reporting by anyone with a cell phone camera and internet connection, plus an increased ease in the ability to manipulate images and messages. "Overall, new media have leveled the playing field between state and non-state actors and made it possible for anyone with minimal access to basic infrastructure – individuals, social movements, criminals and corporations – to operate globally, and often outmaneuver and outpace states and international institutions."[20]

According to JP 3-3.14, "counterdeception includes actions taken to thwart adversary attempts to capitalize on deception tactics."[21] These actions can include efforts to reveal the deception and discredit the deceivers by revealing the truth.[22] In concert with intelligence capabilities to detect deceptions on social media platforms, methods for countering adversary deception need to be envisioned, planned for, and be able to be executed quickly. Even a 24-hour delay can be too long. And, while the deception may be specifically targeted to the US public versus the military, the example with Operation Valhalla demonstrates how targeting the US public can affect the actions of military decision makers.

While the reaction needs to be quick, it also needs to be comprehensive, using all appropriate dissemination mediums, including social media, to get the true story out. Military information support operations (MISO) and PA can be useful in these efforts. As early as 2005, US Central Command (CENTCOM) was using bloggers to spread positive messages and counter false information about US efforts in the Global War on Terrorism. For example, one blogger claimed that US troops lured children with candy and then used them as shields during operations. The CENTCOM PA team of bloggers was able to comment on the blog about the inaccuracy of the information and provide a truthful interpretation of recent events.[23] However,

there is still a predilection by the US military to use traditional media for counterdeception efforts. In discussing counterdeception and exposure of enemy deception operations, JP 3-3.14 expresses that "exposure techniques could include the use of print and broadcast media to garner support among allies and influence the adversary's population."[24]

Another way to thwart adversary social media deceptions is to be less reactionary, instead getting ahead of the enemy in the information war. For example, just as traditional media has been embedded with military units, the United States can use the availability of connectivity to user-generated media to allow airmen, soldiers, seamen, and marines to become the truthful story tellers. The Army has been exploring the use of the new media, and in January 2008, the Army War College held a workshop, "New Media and the Warfighter," that used focus groups to examine opportunities and challenges for new media.[25] As part of the findings, they suggested, "American Soldiers and mil-bloggers can directly and effectively inform the home front by simply telling their stories. For other audiences — including potentially hostile ones — third party validators can be "force multipliers" that enhance the stickiness of U.S. strategic communication and propaganda countering efforts." [26]

Operations Security Concerns

There have already been instances of unofficial military blogs arising out of Iraq and Afghanistan. However, because of its implications for operations security (OPSEC), many have been shut down.[27] OPSEC looks to reduce adversary collection and use of friendly critical information.[28] Social media create a significant threat to this program. For example, in 2010, Israel had to cancel an operation because a soldier posted details about it on his Facebook account. [29] In addition, Israeli leadership encouraged Israeli citizens in the recent Gaza conflict to stop revealing Hamas rocket attack locations on social media because of the potential for the

photographs and descriptions to improve Hamas' targeting ability.[30] Today's military members, raised in the information age, expect constant, open communication.[31] However, this becomes an OPSEC risk. Pictures, with or without geotagging, and seemingly innocuous comments can reveal information on deployments and operations.

OPSEC concerns highlight another area where the US military is vulnerable to enemy social media deception: social engineering. Even members with appropriate privacy settings on sites such as Facebook can become individual targets of deception through phishing.[32] For example, a false Facebook account for US Admiral James Stavridis was discovered while he was serving as the Commander of US European Command and North Atlantic Treaty Organization Supreme Allied Commander in Europe. It appears the profile was used to collect information found on the pages of targeted individuals by "friending" them.[33] A seemingly simple deception was used to collect potentially critical data. In 2011, China's state media reported that the People's Liberation Army would be banned from using social media because of these concerns.[34]

The DOD recognizes its own attempts to enhance strategic communications through social media pose additional deception and OPSEC concerns.[35] Beyond just the open source intelligence (OSINT) that can be collected by other entities, there is also a risk of hacking and deception via computer network operations by allowing .mil networks to be connected to these sites. However, with social media use only expanding, the direction to take is not to restrict its use, but to set up appropriate security protocols and to teach military members to use it responsibly and effectively.[36] While the use of traditional media should not be abandoned, as more and more people are plugged into social media, these platforms have to be utilized for both reactive and proactive counterdeception if the truthful message is going to effectively be conveyed to and imbedded in the minds of both friend and foe.[37]

Opportunities for US Deception

Counterdeception and concerns over OPSEC are not the only areas in which the United States should focus its efforts in regards to social media. These sites can be used in the United States' own MILDEC operations. "See, Think, Do" – this is the target's cognitive process that MILDEC planners strive to exploit. As a technical means, social media can give adversary decision makers a picture that affects their cognitive processing and propels them to act, or not act, in a manner that supports United States' goals and objectives.[38] While a ruse may not be able to be entirely conducted through social media, these platforms can certainly be used as an information conduit, especially as more and more people and organizations become connected to them.[39]

MILDEC operations are generally categorized into two types: ambiguity-reducing and ambiguity-enhancing. The first type attempts to purposefully mislead the adversary, and the second type strives to confuse the adversary.[40] In general, the dawn of the information age created a domain in which ambiguity–enhancing deceptions can be readily employed. [41] Increasing network signals or "noise" via social media can be used to increase ambiguity. Ambiguity-enhancing deceptions are also potentially more resilient to security breaches, as a leak in an already ambiguous operating environment may go unnoticed or further increase uncertainty.[42]

Beyond just increasing information to increase ambiguity, social media's use as a conduit can support tactical and operational deception plans in other ways. For example, it is reported that the US military procured software to allow the development of "realistic" profiles on social media sites.[43] Purported to be used for counterpropaganda, and therefore useful for counterdeception efforts, it could also be used as a conduit to infiltrate and pass on selected

information to the adversary in support of a MILDEC plan. In addition, social media can be used as a modern day conduit for MISO materials in support of a MILDEC operation. For example, messages previously seen via paper pamphlets, such as those used in support of the amphibious buildup before Desert Storm, can be transmitted via blogs, "E-flets," or mass text messaging.[44]

Furthermore, previously mentioned OPSEC concerns are actually one area in which social media can be leveraged for MILDEC operations, specifically by exploiting OPSEC violations. For example, if a unit is deployed to unwittingly support a MILDEC operation, some members may post information on their Facebook pages that reveal location details or operation timelines. These violations by unwitting participants can be exploited, or other "violations" can be created by witting participants, in an effort to mislead or confuse the enemy. Just as the United States would be monitoring social media for OSINT, the adversary will be also.

The DOD may also use social media for deception in support of OPSEC (DISO). One participant in the Army War College's workshop described how he planned operations to look a certain way because he knew individuals would see and blog about it.[45] Thus, if it is known that people are watching, and will blog about it, photograph and post it, or load a video in a social media venue where the adversary will see it, commanders can make equipment, movements, and operations appear a certain way. "DISO can directly support OPSEC by creating numerous false indicators, making it more difficult for adversary intelligence analysts to identify the real indicators that OPSEC is seeking to control."[46] In the Air Force's signature management program, DISO is a key component.[47]

Some may argue that there is too much information and too many collection methods available for social media platforms to be effective to in supporting MILDEC. However, the examples previously described suggest otherwise. Putting a twist on one of the military

deception maxims, "Jones' Dilemma," the 1988 Army Field Manual 90-2, *Battlefield Deception*, states "that the greater the collection capability an opponent has, the greater the opportunity to feed him specifically designed false information."[48] Certainly, the vast number of social media platforms can provide this greater opportunity. But, increased information does not necessarily mislead or confuse if it is implausible or ignored.[49] Therefore, it will take close coordination with intelligence and counterintelligence personnel to determine the most effective means of transferring information. With a good knowledge of the target, social media may be skillfully integrated into a MILDEC operation. For smaller, decentralized terrorist organizations, deceptive information transferred via social media platforms may be more readily performed versus a nation like China whose capabilities are more sophisticated and tightly controlled. However, history has shown that deception success can be achieved by a technologically disadvantaged adversary.[50]

Barriers for Social Media in MILDEC

In regards to MILDEC, concerns with use of social media extend beyond just the OPSEC risk. MILDEC planning and operations are prohibited from targeting or misleading US Congress, US media, and the American public.[51] However, with the openness and global availability of social media, even if the true targets are foreign adversaries, it is difficult to isolate or discriminate between domestic and international audiences.[52] Once the information is out, there is little ability to control where it goes.[53] Increasingly, traditional media is using social media as a source for information, which only magnifies the potential for it to reach American audiences.

Furthermore, the risk of discovery of a US deception operation using social media can have consequences beyond operational degradation; it has a high chance of undermining credibility. "This potential for blowback is especially strong in counterinsurgency and stability

operations. The dilemma is the same people you may need to deceive to protect OPSEC (NGOs, contractors, and especially the indigenous population) are the people that you want to trust you."[54] One brigade combat team commander in Iraq, while completely dedicated to creative IO, believed that deception operations should never be implemented for this reason.[55]

IO also comes with complexity in the level and distribution of authorities, and senior leaders uncomfortable or unfamiliar with social media platforms will be more cautious in their employment.[56] The use of social media is further complicated by the limited clarity and complexity as related to laws for cyberspace. Thomas Wingfield describes how it is necessary to determine the appropriate body of law that governs the information operation action. This may exist under multiple overlapping regimes and at multiple levels. A MILDEC operation may have to consider law not only related to military operations, but at multiple levels: international, domestic, and within an intermediate nation through which the operations runs.[57] For example, if a server for a social media site is held within a neutral country, military operations using this site may violate the rights of neutral nations under the 1907 Hague Convention.[58]

As it specifically relates to MILDEC, one author summarizes that whatever the method utilized, it must be in line with what are traditionally considered "permissible ruses."[59] Unlawful deceptions, including acts of perfidy, extend into the social media realm. Perfidy uses deception to manipulate the enemy's compliance with the laws of war. It includes such acts as feigning surrender to kill or capture the enemy and the use of protective signs and symbols to hide friendly forces or equipment.[60] For example, it would be considered unlawful to use a manipulated YouTube video protraying a false ceasefire in order to capture, injure, or kill the enemy.[61]

The best way to overcome these barriers is already present in IO and MILDEC doctrine. Close coordination of personnel and activities across the IO spectrum, including legal consultants and interagency partners, combined with proactive planning and intelligence preparation of the operational environment can mitigate the risks and barriers associated with social media use.[62] While MILDEC planning and operations should only be revealed on a need-to-know basis, effective communication and collaboration with other IO representatives ensures unity of effort.[63]

The Way Ahead

Social media has already been used in deception and disinformation operations. At a minimum, the United States needs to examine methods for counterdeception, including those that integrate social media. Although the DOD may restrict itself from performing certain deceptions on these forums, feasible tactics and techniques should be explored within MILDEC planning and operations. Four steps can assist in plotting a path to achieve these objectives: embrace, educate, empower, and employ.

Embrace. The first step to integrating social media into MILDEC operations, including counterdeception, is to embrace these technologies. While this process has certainly started, there is more work to be done. In a recent address, the Chairman of the Joint Chiefs of Staff acknowledged the need to embrace change and learn about the increased capabilities for the application of soft power. However, his comments were tinged with typical caution, calling for better understanding to prevent "information fratricide."[64] While this concern is valid, it should not be a block to action, but a call to put more effort into developing tactics, techniques, and procedures (TTPs) for information operations in this realm along with a cadre of experts to execute them.[65]

Educate. Comfort in embracing social media use for MILDEC requires more effort towards development of a cadre of IO experts within all of the services.[66] They should understand social media capabilities, threats, and the strategic implications of its use. Once this occurs, individuals and teams can be integrated into IO cells and individual units. However, more robust education and training is also required for all DOD personnel, including civilian and contractors, on responsible social media use. This includes providing an understanding of the threat of adversary deception tactics, such as social engineering, and the need for overall OPSEC awareness. The training should not be limited to annual computer based training modules. It needs to be integrated into entry level training and professional military education, with targeted advanced education for certain career fields that operate in a high security environment.

Empower. Next, to facilitate agile MILDEC, efforts should be made to allow execution of social media use at lower echelons, especially in terms of counterdeception efforts. This does not mean that any DOD member should be permitted to have an official blog to tell their story. It does mean that the expert IO cadre should be empowered. In "A Commander's Strategy for Social Media," Colonel Thomas Mayfield recommends social media use through centralized planning and decentralized execution.[67] Because the potential exists for negative strategic implications in regards to credibility, information fratricide, and OPSEC, the level of approval authority should remain high to permit integration across all IO areas and government agencies. However, early planning, development of clear commander's intent as to information effects, clear rules of engagement, and TTPs can provide appropriately trained IO personnel with the ability to quickly counter adversary social media deceptions or execute tactical deceptions with these platforms.[68] The negative operational consequences that resulted from the three-day

delayed response after Operation Valhalla illustrates the importance of agility in a world of almost instantaneous information dissemination.

Employment. While PA and MISO, in general operations and for counterdeception, can provide a testing ground for social media use, the DOD should not delay attempts to employ social media for MILDEC. This does not require executing an entire ruse on Facebook through a false profile. As a start, social media can be used as information conduits to targets, showing only pieces of "truthful" information functioning to mislead the adversary. This is similar to the unwitting role of the media during the Desert Storm amphibious landing deception. Exploiting adversary use of social media OSINT through DISO is another lower threat avenue to examine as a starting point. As previously discussed, proactive planning, cooperation with other IO personnel, and careful integration into the supported operation can mitigate many of the risks associated with social media use.

Conclusion

Throughout history, changes in technology have altered the environment and methods for conflict. Today's technologies created cyberspace as the newest warfare environment, with social media as the newest weapon. "The current and future geo-strategic environment requires preparation for a battlespace in which symbolic informational wins may precipitate strategic effects equivalent to, or greater than, lethal operations. It demands a paradigm shift away from an emphasis on information control and towards information engagement."[69] Digital immigrants must learn to adapt to the evolving information warfare capabilities and threats, including the use of social media, or risk failure when trying to obtain and maintain US information superiority.[70]

Challenges exist for the US military in using social media as a weapon in IO. However, as this paper illustrates, adversaries will not be afraid to leverage social media to win the

information battles, including the use of deception and disinformation. At a minimum, counterdeception strategies need to be developed to impede the adversary's ability to capitalize on deception efforts. These strategies should be proactive, rapid when reactive, flexible, and comprehensive, using all possible dissemination methods. However, in order to take full advantage of social media as a weapon, the US military should use these forums as a technical means and conduit in its own MILDEC operations.

The path to maximizing social media's potential in MILDEC starts with integration and collaboration of personnel and efforts across the IO spectrum. It can be further enhanced by creating a culture that *embraces* social media, *educating* military members on its capabilities and security threats, *empowering* IO professionals to use social media, and getting comfortable *employing* social media in IO. Both social media and MILDEC are cost-effective force multipliers.[71] In the current fiscally-constrained environment, it is only sensible to attempt to leverage these capabilities together.

(Notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

[1] Van Der Kleij, De Vries, and Faber, "Opportunities for Social Media in the Comprehensive Approach," 6-4.
[2] Facebook, "Newsroom: Keys Facts," http://newsroom.fb.com/Key-Facts., Twitter, "Twitter Turns Six," http://blog.twitter.com/2012/03/twitter-turns-six.html., YouTube, "Statistics," http://www.youtube.com/t/press_statistics (all accessed 2 December 2012).
[3] Balousha and Conrad, "Israel and Palestinians Wage Social Media War," http://www.dw.de/israel-and-palestinians-wage-social-media-war/a-16397320.
[4] Kruzel, "Pentagon Weighs Social Networking Risks, Benefits," http://www.defense.gov/news/newsarticle.aspx?id=55363.
[5] DOD Directive-Type Memorandum 09-026, "Responsible and Effective Use of Internet-based Capabilities," 2.
[6] DOD, "Social Media Sites,"http://www.defense.gov/registeredsites/SocialMediaSites.aspx (accessed 2 December 12).
[7] MILDEC, ACSC, AY13.
[8] Joint Publication (JP) 3-13, *Information Operations*, II-1.
[9] JP 3-13.4, *Military Deception*, I-1.
[10] Sheehan, "Operational Deception and Modern Warfare," 8-9.
[11] MacKrell, "Contemplating the Counterfactual," 9.
[12] Sheehan, "Operational Deception and Modern Warfare," 9.
[13] Apps, Peter, "Disinformation Flies in Syria's Growing Cyber War," http://www.reuters.com/article/2012/08/07/us-syria-crisis-hacking-idUSBRE8760GI20120807.

[14] Balousha and Conrad, "Israel and Palestinians Wage Social Media War," http://www.dw.de/israel-and-palestinians-wage-social-media-war/a-16397320.
[15] Associated Press, "Tweets of False Shootouts Cause Panic in Mexico City," http://www.foxnews.com/world/2012/09/08/tweets-false-shootouts-cause-panic-in-mexico-city/.
[16] Dauber, "Truth Is Out There," 13-14.
[17] Gertz, "Inside the Ring: Taliban Infiltrate Social Media," http://www.washingtontimes.com/news/2012/aug/22/inside-the-ring-taliban-inflate-social-media/?page=all.
[18] American Free Press, "Web 'Friends' Could Aid Enemy, China's PLA Warns," http://www.google.com/hostednews/afp/article/ALeqM5gAnHp5gfTCxPmdM-WTs5_SJeeTiQ.
[19] Collings and Rohozinski, "Bullets and Blogs," 8.
[20] Ibid.
[21] JP 3-13.4, *Military Deception*, II-2.
[22] Ibid.
[23] Alvarez, "CENTCOM Team Engages Bloggers," http://www.au.af.mil/au/awc/awcgate/dod/20060302_4370.htm.
[24] JP 3-13.4, Military Deception, II-2.
[25] Collings and Rohozinski, "Bullets and Blogs," introductory pages.
[26] Ibid., 4.
[27] Dao, "Pentagon Keeps Wary Watch as Troops Blog," http://www.nytimes.com/2009/09/09/us/09milblogs.html?pagewanted=all&_r=0.
[28] Air Force Instruction (AFI) 10-701, *Operations Security*, 5.
[29] McGregor-Wood, "Facebook Details Force Israeli Military to Cancel Operation," http://abcnews.go.com/International/facebook-details-force-israeli-military-cancel-operation/story?id=10006343.
[30] Balousha and Conrad, "Israel and Palestinians Wage Social Media War," http://www.dw.de/israel-and-palestinians-wage-social-media-war/a-16397320.
[31] Collings and Rohozinski, "Bullets and Blogs," x.
[32] USSTRATCOM, "Social Network Training," http://www.stratcom.mil/snstraining/Social%20Engineering.html (accessed 02 December 2012).
[33] Fitsanakis, "Spies Seen Behind Fake Facebook Profile of Senior NATO Commander," http://intelnews.org/2012/03/12/01-945/.
[34] American Free Press, "Web 'Friends' Could Aid Enemy, China's PLA Warns," http://www.google.com/hostednews/afp/article/ALeqM5gAnHp5gfTCxPmdM-WTs5_SJeeTiQ.
[35] Collings and Rohozinski, "Bullets and Blogs," 5.
[36] Mayfield, "Commander's Strategy for Social Media," 82.
[37] Ibid., 4.
[38] JP 3-13.4, *Military Deception*, I-8, IV-1.
[39] Ibid., GL-3.
[40] Ibid., A-1.
[41] Grohe, "Military Deception: Transparency in the Information Age," 3.
[42] Daniel and Herbig, *Strategic Military Deception*, 17.
[43] Fielding and Cobain, "Revealed: US Spy Operation that Manipulates Social Media," http://www.guardian.co.uk/technology/2011/mar/17/us-spy-operation-social-networks.
[44] MacKrell, "Contemplating the Counterfactual," 8-9, and Kramer, Starr, and Wentz, *Cyberpower and National Security*, 369.
[45] Collings and Rohozinski, "Bullets and Blogs," 61.
[46] JP 3-13.4, *Military Deception*, I-2.
[47] AFI 10-701, *Operations Security*, 15.
[48] Army Field Manual 90-2, *Battlefield Deception*, 1.
[49] Daniel and Herbig, *Strategic Military Deception*, 17-18.
[50] Johnson and Meyeraan, "Military Deception: Hiding the Real—Showing the Fake," 14.
[51] JP 3-13.4, *Military Deception*, II-7.
[52] Keller, "Influence Operations and the Internet," 11.
[53] Collings and Rohozinski, "Bullets and Blogs," 62.
[54] Ibid.
[55] Kramer, Starr, and Wentz, *Cyberpower and National Security*, 364-366.
[56] Kastenberg, "Tactical Level PSYOP and MILDEC Information Operations," 61-71.

[57] Kramer, Starr, and Wentz, *Cyberpower and National Security*, 541.
[58] Keller, "Influence Operations and the Internet," 14.
[59] Kramer, Starr, and Wentz, *Cyberpower and National Security*, 541.
[60] JP 3-13.4, *Military Deception*, I-10.
[61] O'Brien, "Information Operations and the Law of Perfidy," 5.
[62] JP 3-13.4, *Military Deception*, II-3.
[63] Ibid., II-3 and III-5.
[64] Garamore, "Dempsey Discusses Importance of Embracing, Managing Military Change," http://www.defense.gov/News/NewsArticle.aspx?ID=117954.
[65] Keller, "Influence Operations and the Internet," 19.
[66] Kramer, Starr, and Wentz, *Cyberpower and National Security*, 271.
[67] Mayfield, "Commander's Strategy for Social Media," 82.
[68] Collings and Rohonziski, "Bullets and Blogs," 2.
[69] Ibid., 1.
[70] JP 3-13, *Information Operations*, xi.
[71] JP 3-13.4, Military Deception, III-7.

BIBLIOGRAPHY

Air Force Instruction (AFI) 10-701, *Operations Security*, 8 June 2011.

Alvarez, CPT Steve. "CENTCOM Team Engages 'Bloggers'." *American Forces Press Service*, 2 March 2006. http://www.au.af.mil/au/awc/awcgate/dod/20060302_4370.htm.

American Free Press. "Web 'Friends' Could Aid Enemy, China's PLA Warns." *Google.com*, 1 Jun 2011. http://www.google.com/hostednews/afp/article/ALeqM5gAnHp5gfTCxPmdM-WTs5_SJeeTiQ.

Apps, Peter. "Disinformation Flies in Syria's Growing Cyber War." *Reuters.com*, 7 August 2012. http://www.reuters.com/article/2012/08/07/us-syria-crisis-hacking-idUSBRE8760GI20120807.

Army Field Manual 90-2, *Battlefield Deception*, 3 October 1998.

Associated Press. "Tweets of False Shootouts Cause Panic in Mexico City." *FoxNews.com*, 8 September 2012. http://www.foxnews.com/world/2012/09/08/tweets-false-shootouts-cause-panic-in-mexico-city/.

Balousha, Hazem, and Naomi Conrad. "Israel and Palestinians Wage Social Media War." *Deutsche Welle*, 21 November 2012. http://www.dw.de/israel-and-palestinians-wage-social-media-war/a-16397320.

Collings, Deirdre, and Rafal Rohozinski. "Bullets and Blogs: New Media and the Warfighter." Center for Strategic Leadership Workshop Report. Carlisle, PA: Army War College, 2009.

Daniel, Donald C., and Katherine L. Herbig, eds. *Strategic Military Deception*. Elmsford, NY: Permagon Press, 1982.

Dao, James. "Pentagon Keeps Wary Watch as Troops Blog." *New York Times*, 8 September 2009. http://www.nytimes.com/2009/09/09/us/09milblogs.html?pagewanted=all&_r=0.

Dauber, Cori E. "The Truth is Out There: Responding to Insurgent Disinformation and Deception Operations." Military Review LXXXIX, no. 1 (January-February 2009): 13-24. http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20090228_art001.pdf.

Department of Defense (DOD). "Social Media Sites." http://www.defense.gov/registeredsites/SocialMediaSites.aspx (accessed 2 December 12).

DOD Directive-Type Memorandum 09-026. "Responsible and Effective Use of Internet-based Capabilities." Washington, DC: Office of the Deputy Secretary of Defense, 25 February 2010.

Facebook. "Newsroom: Keys Facts." http://newsroom.fb.com/Key-Facts (accessed 2 December 2012).

Fielding, Nick, and Ian Cobain. "Revealed: US Spy Operation that Manipulates Social Media." Guardian, 17 March 2011. http://www.guardian.co.uk/technology/2011/mar/17/us-spy-operation-social-networks.

Fitsanakis, Joseph. "Spies Seen Behind Fake Facebook Profile of Senior NATO Commander." *IntelNews*, 12 March 2012. http://intelnews.org/2012/03/12/01-945/.

Garamone, Jim. "Dempsey Discusses Importance of Embracing, Managing Military Change." *American Forces Press Service*, 20 September 2012. http://www.defense.gov/News/NewsArticle.aspx?ID=117954.

Gertz, Bill. "Inside the Ring: Taliban Infiltrate Social Media." *The Washington Times*, 22 August 2012. http://www.washingtontimes.com/news/2012/aug/22/inside-the-ring-taliban-inflate-social-media/?page=all.

Grohe, LCDR Edwin J. "Military Deception: Transparency in the Information Age." Naval War College Research Report. Newport, RI: Naval War College, November 2007.

Johnson, Maj Mark, and Maj Jessica Meyeraan. "Military Deception: Hiding the Real—Showing the Fake." Joint Forces Staff College Research Report. Norfolk, VA: Joint and Combined Warfighting School, March 2003.

Joint Publication 3-13. *Information Operations*. 13 February 2006.

Joint Publication 3-13.4. *Military Deception*, 26 January 2012.

Kastenberg, MAJ Joshua E. "Tactical Level PSYOP and MILDEC Information Operations: How to Smartly and Lawfully Prime the Battlefield." *The Army Lawyer*, July 2007, 61-71. http://www.loc.gov/rr/frd/Military_Law/pdf/07-2007.pdf.

Keller, Col Rebecca A. "Influence Operations and the Internet: A 21st Century Issue." Air War College Research Report. Maxwell AFB, AL: Air War College, February 2010.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and National Security*. Washington, DC: Potomac Books, Inc., 2009.

Kruzel, John J. "Pentagon Weighs Social Networking Risks, Benefits." *American Forces Press Service*, 4 August 2009. http://www.defense.gov/news/newsarticle.aspx?id=55363.

MacKrell, CDR Eileen F. "Contemplating the Counterfactual: Military Deception in an Age of Perfect Knowledge." Naval War College Research Report. Newport, RI: Naval War College, June 1996.

Mayfield, Thomas D., III. "A Commander's Strategy for Social Media." *Joint Force Quarterly* 60, 1st Quarter (January 2011): 79-83.

McGregor-Wood, Simon. "Facebook Details Force Israeli Military to Cancel Operation." *abcnews.go.com*, 4 March 2010. http://abcnews.go.com/International/facebook-details-force-israeli-military-cancel-operation/story?id=10006343.

O'Brien, CDR Gregory J. "Information Operations and the Law of Perfidy." Naval War College Research Report. Newport, RI: Naval War College, May 2001.

Sheehan, LCDR Francis X. "Operational Deception and Modern Warfare: The Use of Deception in the Information Age." Naval War College Research Report. Newport, RI: Naval War College, February 2000.

Twitter. "Twitter Turns Six." http://blog.twitter.com/2012/03/twitter-turns-six.html (accessed 2 December 2012).

United States Strategic Command (USSTRATCOM). "Social Network Training." http://www.stratcom.mil/snstraining/Social%20Engineering.html (accessed 02 December 2012).

Van Der Kleij, Rick, Arnout De Vries, and Wilco Faber. "Opportunities for Social Media in the Comprehensive Approach." Paper presented at NATO Science and Technology Organization Specialists Meeting. Tallinn, Estonia, April 2012. http://ftp.rta.nato.int/public//PubFullText/RTO/MP/RTO-MP-HFM-201///MP-HFM-201-06.doc.

YouTube. "Statistics." http://www.youtube.com/t/press_statistics (accessed 2 December 2012).